PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-177552
(43)Date of publication of application : 30.06.1998

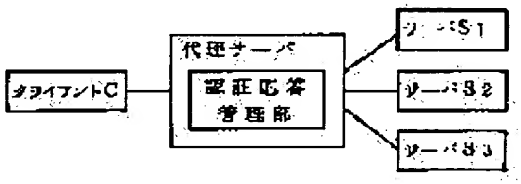
(51)Int.CI. G06F 15/00
G06F 1/00
G06F 13/00

(21)Application number : 08-337260
(22)Date of filing : 17.12.1996

(71)Applicant : FUJI XEROX CO LTD
(72)Inventor : YAMAGUCHI YASUICHIROU

(54) AUTHENTICATION ANSWER METHOD AND AUTHENTICATION ANSWER DEVICE USING THE ANSWER METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To secure the quick operability, to reduce the communication frequency and to attain the use of a terminal of the light specifications such as a PDA, etc., in the communication requiring the authentication information by returning the authentication information requested by a server to this server in place of a client when this client gives an access request to the server.
SOLUTION: This device consists of a client C of a PDA serving as a user terminal, a substitute server which serves as an authentication answer device and a server S which offers various services. The substitute server includes an authentication answer management part which totally controls an authentication answer. In such a constitution, the authentication answer management part collectively manages the authentication information necessary for every server when the client C has an access to the server S. When the client C has an access request to a server S1, for example, the authentication answer management part returns the authentication information requested by the server 1 to this server in place of the client C.



LEGAL STATUS

[Date of request for examination] 17.09.1998
[Date of sending the examiner's decision of rejection] 08.01.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision 2002-01890

of rejection]
[Date of requesting appeal against examiner's decision of rejection] 07.02.2002
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－177552

(43)公開日　平成10年(1998)６月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｃ
	1/00	３７０		1/00	３７０Ｅ
	13/00	３５７		13/00	３５７Ｚ

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願平8－337260

(22)出願日　平成８年(1996)12月17日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　山口　保一郎
神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ＆Ｄビジネスパークビル　富士ゼロックス株式会社内

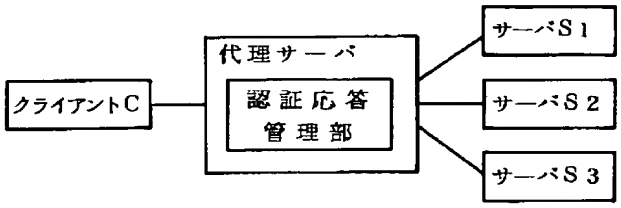
(74)代理人　弁理士　吉田　研二　（外２名）

(54)【発明の名称】　認証応答方法およびその方法を用いた認証応答装置

(57)【要約】

【課題】　複数のサーバにアクセスするとき、それぞれ認証作業が必要だった。これを鍵束のような機構でユーザ端末で管理しても、通信回数が多く、処理の負荷も軽くなかった。

【解決手段】　クライアントＣと複数のサーバＳ１等の間に代理サーバを設ける。この代理サーバは認証応答管理部をもつ。認証応答管理部は、自身がクライアントを認証し、いったん認証したクライアントについて、複数のサーバに対する認証情報の応答を代行する。



1

【特許請求の範囲】

【請求項１】　クライアントからサーバにアクセスするときにサーバごとに必要となる認証情報を一括して管理しておき、クライアントからあるサーバに対するアクセスが要求されたとき、そのクライアントの代わりにそのサーバが求める認証情報をそのサーバに返すことを特徴とする認証応答方法。

【請求項２】　サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置であって、
複数のサーバに対するクライアントの認証情報を保持する保持手段と、
クライアントからあるサーバに対するアクセスの要求があったとき、保持手段からそのサーバに関する認証情報を読み出す読出手段と、
を含み、クライアントに代わってサーバに認証応答をすることを特徴とする認証応答装置。

【請求項３】　該装置自身がクライアントを認証する手段をさらに含み、クライアントが該装置に対して適正な認証情報を返したときに限り、以降クライアントに代わってサーバに認証応答する請求項２に記載の認証応答装置。

【請求項４】　該装置自身がクライアントを認証する手段と、
クライアントが該装置に対して適正な認証情報を返したとき、前記読出手段による読出を許可する許可手段と、
をさらに含み、読み出された認証情報をクライアントに代わってサーバに返す請求項２に記載の認証応答装置。

【請求項５】　所定の条件に従って前記読出手段による読出を禁止する禁止手段をさらに含む請求項４に記載の認証応答装置。

【請求項６】　クライアントから新たなサーバに対するアクセスの要求があったとき、クライアントから送信された該サーバに対する認証情報を前記保持手段に追加登録する登録手段をさらに含む請求項２～５のいずれかに記載の認証応答装置。

【請求項７】　サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置であって、
クライアントに対してサーバとして振る舞うサーバ部と、
サーバに対してクライアントとして振る舞うクライアント部と、
クライアントがサーバにアクセスする際、サーバごとに必要となる認証情報を一括して保持するテーブルとを含み、
前記サーバ部は、
この装置自身がクライアントを認証するための認証手段と、
この認証手段によってクライアントが認証されたとき、このクライアントに関して前記テーブルの読出を許可する許可手段とを含み、

2

前記クライアント部は、
クライアントからあるサーバへのアクセス要求があったとき、このクライアントに関してテーブルの読出が許可されていれば、そのサーバに対する認証情報を読み出す読出手段と、
読み出された認証情報を前記サーバへ送る通信手段と、
を含むことを特徴とする認証応答装置。

【請求項８】　前記サーバ部は、クライアントから新たなサーバに対するアクセス要求があったとき、クライアントから送信された該サーバに対する認証情報を前記テーブルに追加登録する登録手段をさらに含む請求項７に記載の認証応答装置。

【請求項９】　前記サーバ部は、所定の条件に従って前記読出手段による読出を禁止する禁止手段をさらに含む請求項８に記載の認証応答装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、認証応答方法および装置、特に、サーバクライアントシステムにおいてサーバとクライアント間を中継し、サーバの認証要求に対して応答する方法および装置に関する。

【０００２】

【従来の技術】例えばインターネットなどのオープンネットワークでは、フリー（無料）の情報公開がひとつの原則になっている。この原則により、より多くのユーザがより有用な情報に自由にアクセスできる環境が整備、強化されつつある。しかしその一方、例えば契約したユーザのみに特定のサービスを提供したい場合には、サービス提供者と契約者の間で一定のセキュリティ関係を構築する必要がある。この最も簡単な例は、契約者にユーザ名とパスワードなどの認証情報を割り当て、サービスにアクセスする際、これらを入力させる方法である。

【０００３】例えばインターネットでサービスの提供を受ける場合、ユーザはまず画面で所望のサービスを選択する。この要求はサーバに伝えられる。もしそのサーバが、サービスの提供に当たってユーザの認証を行うサーバである場合、ユーザ端末のクライアントに対して認証情報の問合せがなされる。ユーザが認証情報を入力すればこれがサーバに返され、この認証情報が正しければユーザの求めるサービスが提供される。インターネットの利点のひとつは、ユーザがいろいろなサーバから異なるサービスを容易に受けられる点にある。ただしこの場合、通常サーバどうしは互いに独立しているため、サーバごとにクライアントに対して認証情報の入力を要求してくる。

【０００４】図７は、従来のサーバクライアントシステムにおいて、クライアントから異なる２つのサーバに要求が発せられる様子を示している。同図のごとく、まず始めにクライアントＣからサーバＳ１に要求が出される（Ｔ１）。サーバＳ１は認証情報を求めるサーバであ

り、クライアントにその旨の問合せがなされる（Ｔ２）。クライアントはサーバＳ１のための認証情報（ユーザ名Ｕ１とパスワードＰ１）をもって応答する（Ｔ３）。このとき、一般的なブラウザ（情報端末に搭載された情報可視化プログラム、またはそれを搭載した端末）は、認証情報Ｕ１／Ｐ１を自己のバッファに記憶しておく。一方、サーバＳ１は認証情報Ｕ１／Ｐ１を検査し、それらが正しければ、求められたサービスをクライアントに提供する（Ｔ４）。

【０００５】つづいて、クライアントＣが別のサーバＳ２にサービスを要求する（Ｔ５）。サーバが変わったことは、ユーザは特に意識しない。要求の送付にあたり、ブラウザはバッファに記憶していた認証情報Ｕ１／Ｐ１をサーバ名Ｓ２に付して送付する。この認証情報はサーバＳ１に対するものであってサーバＳ２にとっては適正ではないため、サーバＳ２から独自に認証情報の問合せがなされる（Ｔ６）。クライアントはサーバＳ２のための認証情報Ｕ２／Ｐ２を入力しなおして応答する（Ｔ７）。サーバＳ２は認証情報Ｕ２／Ｐ２の確認後、クライアントにサービスを提供する（Ｔ８）。

【０００６】以上、このシステムでは、サーバが変わるたびに認証情報の問合せと入力が必要になる。この煩わしさを回避するために、「Ｍａｃｉｎｔｏｓｈ漢字Ｔａｌｋ７．５、アップグレードガイド」のｐ２２～２６に、単一のパスワードによってネットワーク上の複数のサービスが受けられる「鍵束」という機能が説明されている。すなわち、サービスごとに異なる鍵を束の状態で管理し、この鍵束に対して固有のパスワードを設けるというもので、このパスワードを入れさえすればサービスに応じて必要な鍵が鍵束から選択され、これがサーバに渡される。

【０００７】

【発明が解決しようとする課題】上述の鍵束に関する機能はユーザの端末に搭載されるソフトウエアで実現される。この従来技術の場合、以下の点で改善の余地が認められる。

【０００８】１．ユーザがパスワードを入れる回数は減るが、クライアントとサーバ間の通信回数が減らない。例えば、図７の一連の通信において、Ｔ３とＴ７における認証情報のユーザによる入力がなくなるが、問合せと応答自体は必要であり、図７と同じ通信回数になる。このため、通信コストの低減に結びつかないだけでなく、サービスの迅速性が阻害される。

【０００９】２．ユーザの端末がＰＤＡ（Personal Digital Assistance）など比較的軽いハードウエア仕様である場合、複数のサーバに対するアクセスを管理し、実行する一連の処理の負荷が重い。このため、処理の即時性に欠けることがある。

【００１０】３．鍵束の機能を実現するために、ユーザの端末に手を加えなければならない。

【００１１】本発明は以上の課題に鑑みてなされたものであり、その目的は、認証情報を必要とする通信における迅速性を確保し、通信回数を低減し、ＰＤＡなど軽い仕様の端末でも実現可能であり、その端末に手を加える必要のない認証応答方法および装置を提供することにある。

【００１２】

【課題を解決するための手段】本発明の認証応答方法は、クライアントからサーバにアクセスするときにサーバごとに必要となる認証情報を一括して管理しておき、クライアントからあるサーバに対するアクセスが要求されたとき、そのクライアントの代わりにそのサーバが求める認証情報をそのサーバに返すものである。この方法によれば、認証情報の問合せと応答がクライアントとサーバ間ではなく、認証情報の管理主体とサーバ間に発生する。このため、クライアントは応答の義務から開放され、通信回数が減る。また、クライアントが応答しなくてよいため、ＰＤＡなど、軽い仕様の端末で処理上なんら問題は生じない。端末に新たな機能を追加する必要もなく、管理主体に認証情報の一括管理機能を設ければ足りる。

【００１３】一方、本発明の認証応答装置は、サーバクライアントシステムにおいてクライアントと複数のサーバを中継する装置である。この装置は、複数のサーバに対するクライアントの認証情報を保持する保持手段（２０）と、クライアントからあるサーバに対するアクセスの要求があったとき、保持手段からそのサーバに関する認証情報を読み出す読出手段（３６）とを含み、クライアントに代わってサーバに認証応答をする。この装置では、クライアントの認証情報が保持手段に記憶されているため、クライアントが例えばサーバＳ１にアクセスしたければ、読出手段が保持手段からこのクライアントのサーバＳ１に関する認証情報（例えばＵ１／Ｐ１）を読み出す。つづいてこれをサーバＳ１に送る。このため、クライアントは認証応答から開放され、上述の認証応答方法同様の効果が得られる。

【００１４】本発明の認証応答装置はさらに、この装置自身がクライアントを認証する手段（３２）と、クライアントが該装置に対して適正な認証情報を返したとき、前記読出手段による読出を許可する許可手段（３４）とを含んでもよい。つまり、サーバＳ１などへのアクセスに先立ち、この装置が自らクライアントを認証する。ここで正しい認証情報が入力されれば、以降、サーバＳ１等に対する認証応答を代行する。この構成よれば、ユーザは認証情報を管理する装置があることを知り、これを積極的に活用することができる。

【００１５】本発明の認証応答装置はさらに、所定の条件に従って前記読出手段による読出を禁止する禁止手段（３８）を含んでもよい。この構成によれば、例えば一定期間ごとに読出を禁止することにより、セキュリティ

のレベルを初期状態に戻すことができる。

【００１６】本発明の認証応答装置はさらに、クライアントから新たなサーバに対するアクセス要求があったとき、クライアントから送信された該サーバに対する認証情報を前記保持手段に追加登録する登録手段（４０）を含んでもよい。新たなサーバについて、保持手段はそのサーバ用の認証情報をもっていない。したがって、クライアントは認証情報を入力せざるを得ず、これがサーバに伝えられる。このとき、この認証情報を捕捉して保持手段に書き込んでしまうのである。この構成によれば、保持手段の保守作業の労力を軽減することができる。

【００１７】本発明の認証応答装置の別の態様は、クライアントに対してサーバとして振る舞うサーバ部（１６）と、サーバに対してクライアントとして振る舞うクライアント部（１８）と、クライアントがサーバにアクセスする際、サーバごとに必要となる認証情報を一括して保持するテーブル（２０）とを含み、前記サーバ部は、この装置自身がクライアントを認証するための認証手段（３２）と、この認証手段によってクライアントが認証されたとき、このクライアントに関して前記テーブルの読出を許可する許可手段（３４）とを含み、前記クライアント部は、クライアントからあるサーバへのアクセス要求があったとき、このクライアントに関してテーブルの読出が許可されていれば、そのサーバに対する認証情報を読み出す読出手段（３６）と、読み出された認証情報をサーバに送る通信手段（１４）とを含む。

【００１８】この構成おいて、サーバ部の認証手段がまずクライアントを認証する。認証の後、許可手段により、そのクライアントに関してテーブルの読出が許可される。この後、このクライアントからあるサーバへのアクセス要求があったとき、読出手段によって、そのサーバに対する認証情報が読み出される。読み出された認証情報はサーバに送られる。このため、上述の認証応答方法同様の効果が得られる。

【００１９】

【発明の実施の形態】本発明の好適な実施形態を適宜図面を参照しながら説明する。以下、認証情報はユーザ名とパスワードで構成されるものとし、前者をＵ、後者をＰと総括的に表記する。同様にサーバをＳと表記し、ユーザＵｉのサーバＳｊに対する正しい認証情報は、Ｕｉｊ／Ｐｉｊであるとする。添え字は説明上必要なときに付する。

【００２０】図１は本発明の認証応答装置を用いるシステムの概念的な構成図である。同図のごとくこのシステムは、ユーザの端末であるＰＤＡのクライアントＣと、認証応答装置である代理（プロキシー）サーバと、各種サービスを提供するサーバＳからなる。代理サーバは認証応答全般を司る認証応答管理部を含む。代理サーバは便宜上サーバＳ０とし、クライアントＣはユーザＵ０であるとする。したがって、このクライアントＣの代理サーバに対する認証情報は、Ｕ００／Ｐ００である。なお、同図ではクライアントＣがひとつしか存在しないが、実際には多数存在することが考えられる。

【００２１】この構成において、認証応答管理部は、クライアントＣがサーバＳにアクセスするときサーバごとに必要となる認証情報を一括して管理している。クライアントＣからあるサーバへのアクセスが要求されたとき、認証応答管理部はクライアントＣに代わってそのサーバが求める認証情報をそのサーバに返す。

【００２２】図２は代理サーバの内部構成を示す。代理サーバは、クライアントＣと要求および応答を通信する第一通信部１２、認証応答管理部１０、サーバＳと要求および応答を通信する第二通信部１４を含む。

【００２３】認証応答管理部１０は、クライアントＣからサーバに見えるサーバ部１６と、サーバＳからクライアントに見えるクライアント部１８と、認証情報をクライアント別に記憶するテーブル２０を含む。

【００２４】サーバ部１６は、第一通信部１２を介してクライアントＣからの送信内容を受ける受付部３０と、代理サーバが自己のためにクライアントＣを認証する認証部３２と、認証部３２の認証結果にもとづき、テーブル２０からの読出をクライアントごとに許可する読出許可部３４と、所定の条件にしたがってテーブル２０からの読出を禁止する読出禁止部３８と、クライアントＣから新たなサーバに対するアクセスが要求されたとき、そのサーバに必要な認証情報をクライアントＣの送信内容から抽出してテーブル２０に追加登録する登録部４０と、３つの方向、すなわち認証部３２、後述のクライアント部１８の読出制御部３６およびクライアント部１８の受付部６２からのメッセージ等のデータを切り替えて第一通信部１２へ送り出す切替部５４を含む。登録部４０における登録のためには、ユーザ名の他に、当然ながら目的のサーバに対するそのユーザの認証情報が必要である。

【００２５】認証部３２は、クライアントＣからの送信内容がテーブル２０に対する新たな認証情報の登録を指示しているか否かを検査する登録指示検出部４２と、テーブル２０を走査してクライアントＣの代理サーバに対する認証情報が正しいか否かを検査する認証検査部４４を含む。読出禁止部３８は、クライアントごとに禁止条件が満たされているか否かを確認する禁止管理部５０と、その指示によってクライアントごとに読出を禁止する個別読出禁止部５２を含む。

【００２６】一方、クライアント部１８は、実際にテーブル２０からの読出を制御する読出制御部３６と、読み出されたデータを受け付け、これを第二通信部１４に送る送出部６０と、サーバＳから第二通信部１４を介してその送信内容を受ける受付部６２を含む。読出制御部３６はさらに、読み出すべきクライアントのデータを検索する検索部４６と、そのクライアントに関するデータが

読出許可状態にあるか否かを検査する許否検査部４８を含む。

【００２７】図３はテーブル２０の詳細を示す構成図である。同図のごとくテーブル２０は、クライアントごと、すなわちユーザＵ０～Ｕｎに分割された複数のブロック７０の集合体である。各ブロック７０には、Ｕ０等のユーザ名７２、そのブロック７０の読出の許可、禁止状態をそれぞれ「○」「×」で示す許否フラグ７４、サーバ名７６、認証情報７８の各領域をもつ。例えばユーザＵ０の場合、サーバＳ０等に対する認証情報がＵ００／Ｐ００等と記憶されている。ユーザＵ０のブロックの許否フラグは「○」であり、テーブル２０において、少なくともこのユーザのブロック７０は読出許可状態にあることがわかる。許否フラグ７４は初期状態ではすべて「×」である。以下、ユーザＵ０がいろいろなサーバへアクセスする際の代理サーバの動作を説明する。

【００２８】１．認証情報が記憶されている複数サーバへの連続アクセス

図４はクライアントＣに当たるユーザＵ０がサーバＳ１、Ｓ２に対してつづけてアクセスする通信の手順を示している。同図のごとく、まず始めにクライアントＣから代理サーバＳ０に対して、「サーバＳ１にアクセスしたい」旨の要求が送出される（Ｔ１）。この要求は、クライアントＣを特定する「Ｕ０」および目的のサーバＳ１を特定する「Ｓ１」の２つのパラメータで構成される。これらのパラメータは図２の第一通信部１２を介してサーバ部１６の受付部３０で受け取られ、クライアント部１８の読出制御部３６へ送られる。このとき、パラメータには認証情報（Ｕ００／Ｐ００等）が含まれていないため、認証部３２は動作しない。

【００２９】読出制御部３６の検索部４６は、ユーザ名であるＵ０をキーとしてテーブル２０に検索をかける。その結果、図３の最も左側のブロックが発見される。つづいて許否検査部４８がそのブロックの許否フラグ７４の状態を確かめる。この場合、まだ初期状態で「×」であるから、「読出は禁止」と判断される。このため目的のサーバＳ１が必要とする認証情報を読み出すことはできず、代理サーバＳ０としては、まずこのユーザＵ０を自装置で認証する必要があること知る。そこで、読出制御部３６は切替部５４に対し、

「代理サーバＳ０に対する認証情報を入力してください」

というメッセージを送る。切替部５４はこのメッセージを第一通信部１２を介してクライアントＣへ送り、認証情報を問い合わせる（Ｔ２）。クライアントＣは端末の画面にこのメッセージを表示し、ユーザは代理サーバＳ０に対する自己の認証情報「Ｕ００／Ｐ００」を入力する。この認証情報は、すでに判明している目的サーバ名「Ｓ１」と組み合わされ、第一通信部１２を介して受付部３０に送られ、認証部３２へ回送される（Ｔ３の前半）。

【００３０】認証部３２では、まず登録指示検出部４２がこのパラメータ「Ｓ１／Ｕ００／Ｐ００」を判読する。この場合、Ｓ１は新たなサーバではないため、登録の指示ではないと判断され、登録部４０は動作しない。つづいて認証検査部４４が、パラメータＵ００／Ｐ００をテーブル２０に照合し、代理サーバＳ０に対するユーザＵ０の正しい認証情報であるか否かを確認する。Ｕ００／Ｐ００はテーブル２０のユーザＵ０用ブロックのサーバＳ０に対する認証情報と一致するため、「正しい」旨が読出許可部３４に通知される。読出許可部３４は、ユーザＵ０のブロック７０の許否フラグ７４を「×」から「○」に変更し、以降の読出を許可する。なお、代理サーバＳ０に対する誤った認証情報が入力された場合は、入力部３２から「もういちど入力してください」などのエラーメッセージが切替部５４に送られ、これがクライアントＣに送付される。

【００３１】つぎに、読出制御部３６の検索部４６がユーザＵ０のブロック７０を検索し、許否検査部４８がそのブロック７０の許否フラグ７４を検査する。ここでは「○」に変更されているため、目的サーバ名「Ｓ１」に対応する認証情報「Ｕ０１／Ｐ０１」が読み出される。このとき、許否フラグが確実に「○」に変更されるまで検査を待たせる趣旨で、必要に応じて検査を遅延させてもよい。読み出されたパラメータ「Ｕ０１／Ｐ０１」はクライアント部１８の送出部６０に送られ、第二通信部１４を介してサーバＳ１にアクセス要求として送り出される（Ｔ３の後半）。

【００３２】サーバＳ１では、ユーザＵ０からの最初のアクセスであるにも拘らず必要な認証情報が正しく与えられたため、認証情報の問合せをスキップし、要求されたサービスを提供する。サービスを実現するデータは第二通信部１４を経てクライアント部１８の受付部６２で受け取られ、切替部５４に向けて出力される。切替部５４はこのデータを第一通信部１２を介してクライアントＣへ送付する（Ｔ４）。以上が最初のサーバに対するアクセスである。

【００３３】つづいてクライアントＣは、代理サーバＳ０に対し、別のサーバＳ２に対するアクセスの要求を送る（Ｔ５の前半）。この要求はクライアントＣを特定する「Ｕ０」と目的のサーバを特定する「Ｓ２」の２つのパラメータで構成される。これらのパラメータはサーバ部１６の受付部３０からクライアント部１８の読出制御部３６へ送られる。このときもパラメータに認証情報が含まれていないため、認証部３２は動作しない。読出制御部３６の検索部４６はユーザＵ０用のブロック７０を見つけ、許否検査部４８が許否フラグ７４の状態を確かめる。この場合、すでに「○」、すなわち読出許可状態にあるため、目的サーバ名「Ｓ２」に対応する認証情報「Ｕ０２／Ｐ０２」が読み出される。このパラメータは

クライアント部１８の送出部６０に送られ、第二通信部１４を介してサーバＳ１にアクセス要求として送り出される（Ｔ５の後半）。以下、サーバＳ２によるサービスの提供（Ｔ６）はＴ４同様である。

【００３４】なお、セキュリティを考えた場合、いったん読出許可状態になったブロック７０が以降無条件でその状態を保つことは望ましくない。このため、読出禁止部３８は読出許可状態にあるブロックを再度禁止状態にもどす。禁止管理部５０は禁止状態にもどすための条件を管理しており、例えば一連のセッションが終了したときや、一定期間クライアントからサーバへのアクセスがない場合など、ある条件が満たされたとき、禁止すべきブロック７０を個別読出禁止部５２へ通知する。個別読出禁止部５２は、通知されたブロック７０の許否フラグ７４を「○」から「×」に戻す。

【００３５】以上、本実施の形態によれば、図７の通信手順に比べてクライアントＣとサーバＳ１、Ｓ２の通信回数を減らすことができる。これは代理サーバＳ０がサーバＳ１、Ｓ２に代わってクライアントの認証を行い、クライアントに代わってサーバＳ１、Ｓ２への認証応答を行うためである。また本実施の形態によれば、異なる認証情報が一括管理、応答されるため、サーバが変わるたびにユーザがいちいち認証情報を入れなおす必要がなくなる。例えば図４の場合、以降クライアントＣがサーバＳ１、Ｓ２を交互にアクセスするときでも、もはや認証情報の入力はいっさい不要である。このため、さらに図７の場合との差が大きくなる。本実施の形態では、ユーザの端末であるＰＤＡなどで鍵束を管理する必要がなく、端末側の処理負荷が軽くなる。また、代理サーバのみに手を加えればよいため、既存のサーバやクライアントに変更もいらない。代理サーバひとつで多数のクライアント、サーバをカバーできるため、本実施の形態は実施の際も効率的である。

【００３６】２．認証情報の不要なサーバへのアクセス

サーバの中には認証情報を求めないものも多数存在する。そうしたサーバへのアクセスを図５によって説明する。同図において、ユーザＵ０はサーバＳ３へアクセスしたいとする。アクセスの要求（Ｔ１）、代理サーバＳ０からの認証情報の問合せ（Ｔ２）、それに対する応答（Ｔ３の前半）までは図４同等である。応答の結果、認証情報「Ｕ００／Ｐ００」と目的サーバ名「Ｓ３」が組み合わされ、認証部３２へ送られる。

【００３７】認証部３２は、パラメータＵ００／Ｐ００が正しい認証情報であるため、ユーザＵ０のブロックの許否フラグ７４を「×」から「○」に変更する。つぎに読出制御部３６は、ユーザＵ０のブロック７０が読出許可状態にあることを知り、目的サーバ名「Ｓ３」に対応する認証情報を読み出そうとする。しかし、図３のごとくユーザＵ０のブロック７０にはサーバＳ３の名前がない。この状況は、

（１）認証情報の必要な新たなサーバに対するアクセス
（２）認証情報の不要な新たなサーバに対するアクセス

のいずれかが発生していることを意味する。（１）の場合はクライアントに認証情報を問合せなければならない。しかし、（２）の場合は不要であり、問合せはシステムの動作として不適切である。そこで読出制御部３６は、まず（２）を想定し、読出の結果として形式的に「無（ｎｕｌｌ）」を送出部６０に送る。したがって、第二通信部１４からサーバＳ３にはアクセスの要求のみが送り出される（Ｔ３の後半）。一方、サーバＳ３は要求があってもユーザの認証を行わないため、無条件でサービスを提供する（Ｔ４）。

【００３８】以上が認証情報を求めないサーバへのアクセスである。ここでは、まずＴ２において代理サーバＳ０自身がユーザの認証を行ったが、別の手順もある。例えば、サーバＳ３に対するアクセス要求を認証情報の有無に関係なく直接サーバＳ３に送ってもよい。その場合、要求に対してサーバＳ３がサービスを提供するという単純な通信手順で済む。この方法の場合、目的のサーバが認証情報を求めるサーバであれば、そのサーバがユーザ名とパスワードの入力を求めてくることになる。そのときに代理サーバが自己に対する認証情報の送付をクライアントに対して求める構成としてもよい。

【００３９】３．認証情報が必要だが未登録のサーバへのアクセス

テーブル２０に登録されていない新たなサーバであり、しかもそのサーバが認証情報を要求する場合がある。図６はそうした場合の通信手順を示している。

【００４０】同図において、ユーザＵ０はサーバＳ３へアクセスしたいとする。アクセスの要求（Ｔ１）、代理サーバＳ０からの認証情報の問合せ（Ｔ２）、それに対する応答（Ｔ３の前半）、パラメータＳ３に基づくサーバＳ３への要求（Ｔ３の後半）については図５同等である。要求を受けたサーバＳ３には、自己が必要とする認証情報が与えられないため、認証情報の問合せを行う（Ｔ４）。

【００４１】この問合せに対し、ユーザがサーバＳ３のための認証情報Ｕ０３／Ｐ０３を入力する。この認証情報は代理サーバの認証部３２へ与えられる。認証部３２の登録指示検出部４２は、新たなサーバ名が認証情報を伴う形で送られてきたことを確認し、これを新たな登録の指示とみなして登録部４０にパラメータＳ３／Ｕ０３／Ｐ０３を送る。登録部４０は、テーブル２０のユーザＵ０のブロックに新たなサーバＳ３の欄を設け、認証情報Ｕ０３／Ｐ０３を書き込む。以上が登録動作である。

【００４２】一方、読出制御部３６はサーバ名「Ｓ３」をキーとして認証情報Ｕ０３／Ｐ０３を読み出し、これをクライアント部１８等を介してサーバＳ３に送る（Ｔ５の後半）。サーバＳ３は正しい認証情報が与えられことを確認し、求められたサービスを提供する（Ｔ６）。

11

【００４３】以上がサーバの登録を伴う通信である。この方法によれば、ユーザが新たなサービスを受けるようになったとき、そのための認証情報を自動的にテーブル２０へ追加していくことができる。その結果、テーブル保守の作業工数を大幅に軽減することができる。

【図面の簡単な説明】

【図１】　本発明の認証応答装置を用いるシステムの概念的な構成図である。

【図２】　実施の形態の代理サーバの内部構成図である。

【図３】　図２のテーブルの詳細を示す構成図である。

【図４】　ユーザＵ０がサーバＳ１、Ｓ２に対してつづけてアクセスする通信の手順を示す図である。

【図５】　認証情報を求めないサーバへのアクセスの通信手順を示す図である。

12

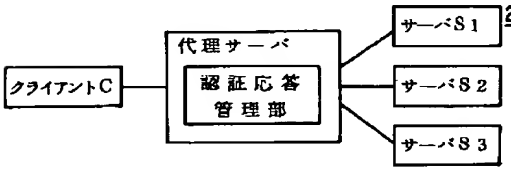
【図６】　認証情報が必要だが未登録のサーバへのアクセスの通信手順を示す図である。

【図７】　従来のサーバクライアントシステムにおいて、クライアントから異なる２つのサーバがアクセスされる様子を示す図である。

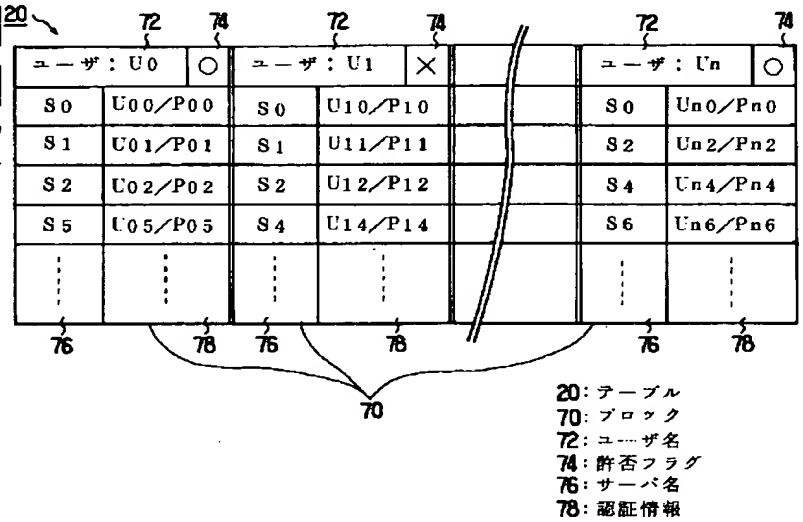
【符号の説明】

１０　認証応答管理部、１２　第一通信部、１４　第二通信部、１６　サーバ部、１８　クライアント部、２０　テーブル、３０　受付部、３２　認証部、３４　読出許可部、３６　読出制御部、３８　読出禁止部、４０　登録部、４２登録指示検出部、４４　認証検査部、４６　検索部、４８　許否検査部、５０禁止管理部、５２　個別読出禁止部、６０　送出部、６２　受付部、７０　ブロック、７２　ユーザ名、７４　許否フラグ、７６　サーバ名、７８　認証情報。

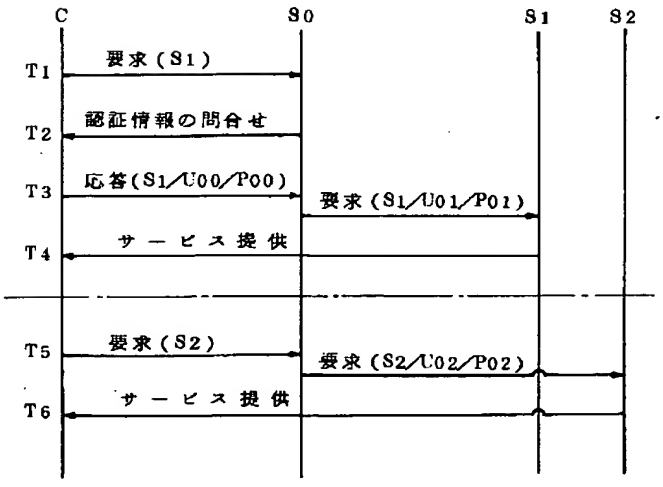
【図１】



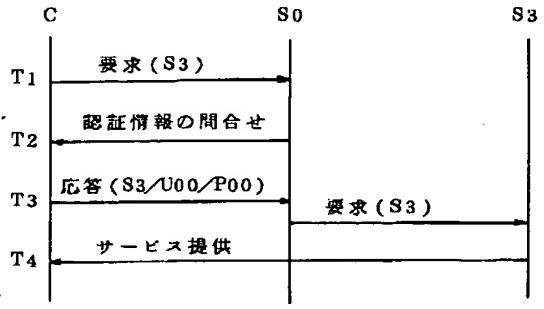
【図３】



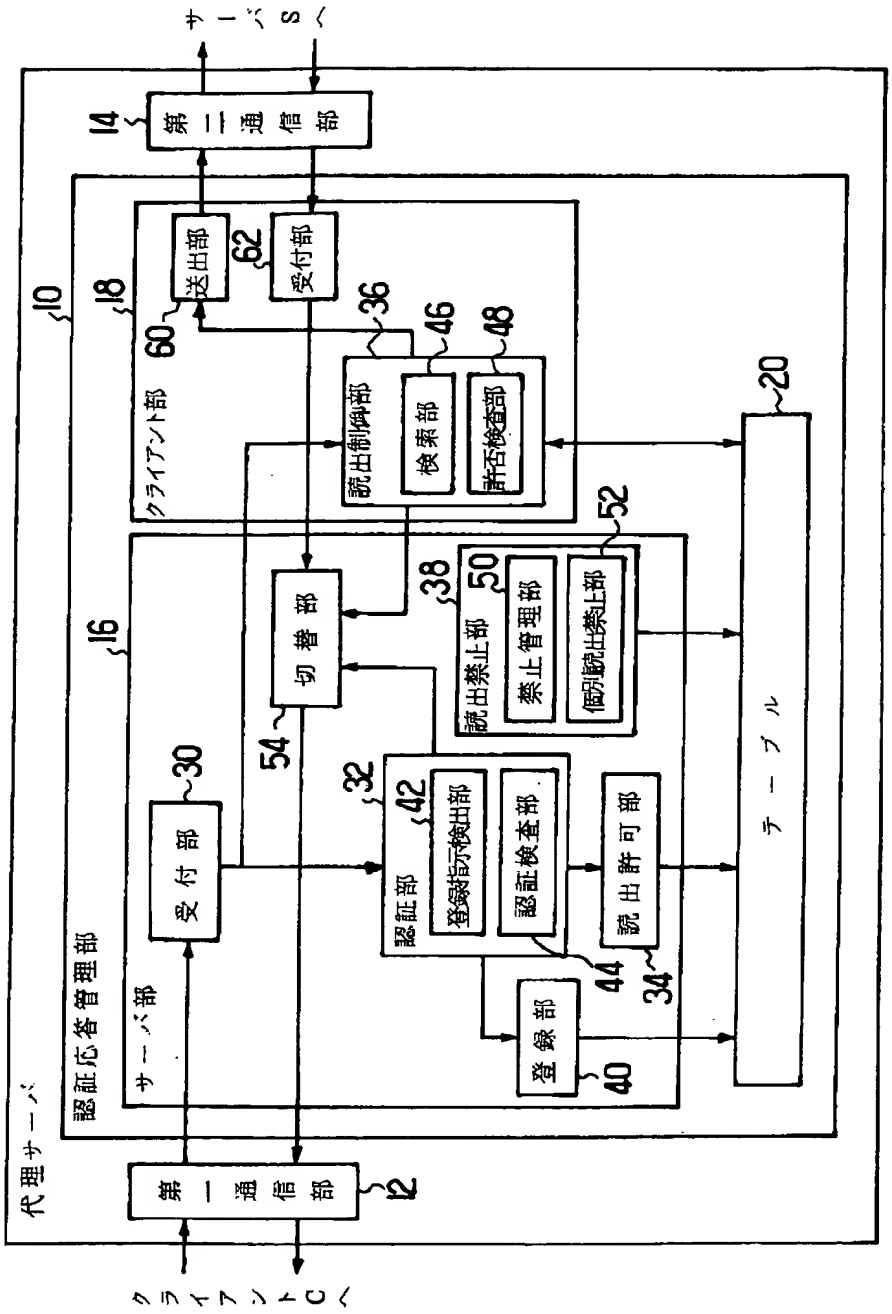
【図４】



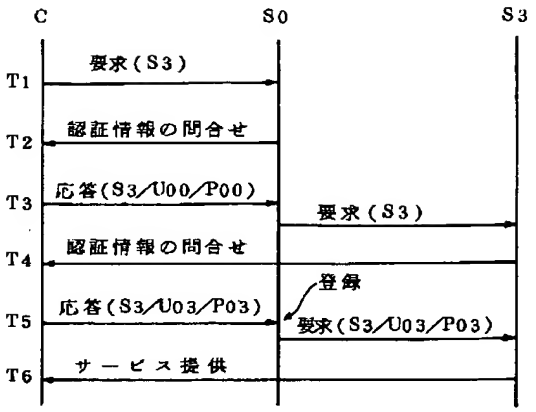
【図５】



【図２】

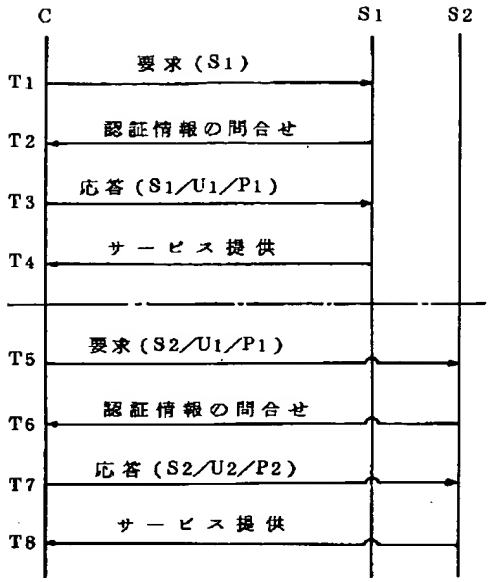

サーバS
第二通信部
14
10
18
送出部
62
受付部
60
クライアント部
36
46
48
読出制御部
検索部
許否検査部
20
52
16
切替部
38
50
読出禁止部
禁止管理部
個別読出禁止部
テーブル
54
30
32
42
受付部
認証部
登録指示検出部
認証検査部
読出許可部
44
34
登録部
40
認証応答管理部
サーバ部
代理サーバ
第一通信部
12
クライアントC

【図６】


C
S0
S3
T1
要求(S3)
T2
認証情報の問合せ
T3
応答(S3/U00/P00)
要求(S3)
T4
認証情報の問合せ
登録
T5
応答(S3/U03/P03)
要求(S3/U03/P03)
T6
サービス提供

【図７】

従　来　技　術


C
S1
S2
T1
要求(S1)
T2
認証情報の問合せ
T3
応答(S1/U1/P1)
T4
サービス提供
T5
要求(S2/U1/P1)
T6
認証情報の問合せ
T7
応答(S2/U2/P2)
T8
サービス提供